Dr.WEB®
dal 1992

Proteggi ciò che hai creato

Chi è cieco non teme il serpente

Attenti alla minaccia: Carberp, un trojan bancario!

La storia di come un computer aziendale è stato infettato da Trojan.Carberp

Questa è una storia vera ed è successa nel dicembre 2012 in un'azienda a Mosca.

1. Un'addetta alla contabilità accede a Internet da un computer aziendale su cui è installato un sistema di home banking e legge articoli su un sito web dedicato al benessere e alla salute femminile.
2. Il browser si blocca, poi appare una finestra di avviso di mancato funzionamento.
3. La dipendente preme su uno dei pulsanti nella finestra per farla sparire e per continuare la lettura dell'articolo.
4. Tuttavia il browser non funziona, perciò la dipendente chiama l'amministratore di sistema.
5. L'amministratore di sistema accede al computer in questione utilizzando la sua password di amministratore di DOMINIO e risolve il problema che bloccava il browser – quindi si può continuare a leggere quell'articolo tanto "importante". Il trojan che si è infiltrato sul PC dell'addetta alla contabilità SENZA FARSI NOTARE è stato attivato dalla dipendente stessa (che aveva cliccato su un pulsante nella finestra del browser, come nel passo 3 sopra). A questo punto, la password dell'intera rete locale e la password del sistema di home banking sono già nelle mani dei truffatori.
6. L'addetta alla contabilità non usa il sistema di home banking per alcuni giorni, ma durante questo periodo vengono eseguite una serie di transazioni fraudolente di un importo considerevole.

Al trojan bancario **Carberp** bastano da uno a tre minuti per rubare le password e il denaro dal conto della vittima.

Che cosa sono i trojan bancari?

Sono malware molto pericolosi che possono:

- rubare password di accesso ai sistemi di home banking e di pagamento e denaro dai conti bancari di piccole e grandi aziende;
- scaricare sul computer altri programmi dannosi e i loro moduli aggiuntivi;
- bloccare completamente l'utilizzo del computer secondo un comando opportuno impartito dai malintenzionati su remoto.

Attualmente il trojan bancario più pericoloso è **Trojan.Carberp**.

Questo cavallo di troia possiede versioni adatte al furto di fondi da tutti i sistemi di home banking più comuni.

Attenzione! Le piccole e medie imprese corrono il rischio maggiore a causa del modo utilizzato dai truffatori per infettare computer.

Che cosa ruba un trojan bancario?

Soldi. Nient'altro interessa ai truffatori.

Il possessore del trojan dispone di informazioni complete riguardanti il conto della vittima e può accedere a qualsiasi dato sul computer infetto.

Prima di cominciare il furto, i possessori del trojan raccolgono informazioni riguardanti la loro vittima: in qualsiasi momento conoscono molto precisamente il saldo del conto dell'azienda, gli importi e le causali delle transazioni (le stesse causali si usano poi per falsificare ordini di pagamento) e ricevono informazioni istantanee su TUTTI i pagamenti effettuati dal contabile dell'azienda. L'azienda vittima viene seguita giorno e notte prima che il contro venga svuotato. I truffatori ottengono i seguenti dati:

Se è stata rubata la password del sistema di home banking

- Conto bancario
- Saldo del conto bancario
- Importo del bonifico bancario (somma accreditata)
- Motivo di pagamento
- Sistema di home banking compromesso (nome)
- Indirizzo WWW del sistema di home banking
- Indirizzo IP del computer vittima
- Browser in uso

Se è stata compromessa una carta bancaria

- BIN della banca
- Conto bancario della vittima
- Indirizzo del sistema di pagamento elettronico in cui la carta bancaria è stata compromessa
- Numero della carta bancaria
- Scadenza della carta bancaria
- Nome e cognome del titolare della carta bancaria
- CVV2/CVC2

A chi giova?

I malware moderni vengono creati da scrittori di virus professionisti. La produzione di malware oggi è un'organizzazione criminale ben strutturata che coinvolge programmatori altamente qualificati, capaci di sviluppare software di sistema e applicazioni.

Un trojan bancario viene sviluppato e distribuito da un gruppo criminale organizzato. Gli sviluppatori lavorano in un paese, i server da cui si diffonde il trojan sono locati in un altro paese, gli organizzatori agiscono da un altro paese ancora, mentre i "partner", cioè criminali che comprano i servizi dei possessori di **Trojan.Carberp** e mantengono la botnet del programma maligno per commettere furti si trovano in più paesi.

Il codice del cavallo di troia viene perfezionato continuamente dai suoi autori, le nuove versioni vengono rilasciate in modo regolare. Ogni giorno i database virali di Dr.Web vengono completati con alcune decine di varietà di **Trojan.Carberp**!!!!! E questo è solo uno dei moltissimi cavalli di troia...

Fatti

- Ogni giorno il laboratorio antivirale di Doctor Web riceve in media 60 000 esemplari di programmi malevoli.
- Il 28 novembre 2012 è stato una sorta di record – oltre 300 000 esemplari di programmi malevoli sono stati inviati al laboratorio per essere analizzati. Questo record è stato superato a dicembre 2012 con una cifra raddoppiata! E con queste cifre non si esaurisce il numero di codici dannosi creati nell'arco di un giorno.

Gli analisti antivirali non possiedono poteri magici e non possono esaminare subito diverse migliaia di file sospetti che arrivano ogni giorno. Perciò vi è sempre un rischio che l'elaboratore si infetti da una minaccia ancora non conosciuta dall'antivirus.

Il trojan è sopraggiunto senza farsi notare?

Il trojan **non Vi ha colto all'improvviso**! L'AVETE TROVATO VOI STESSI.

I trojan dalla famiglia Trojan.Carberp penetrano sui computer **mentre l'utente visita siti web violati**. Non è necessaria un'azione da parte dell'utente per far passare il virus perché **l'infezione avviene automaticamente**.

Siti web che più spesso sono fonti di malware:

1. 1.Siti di tecnologia e di telecomunicazione.
2. Portali di notizie, forum e siti riguardanti la contabilità, corsi di formazione e lezioni on-line.
3. Siti femminili (dedicati al benessere, alla salute e cucina).

Un'altra via di infezione molto diffusa è quando virus si infiltrano sul computer da supporti rimovibili.

Attenzione!

Supporti rimovibili sono non solo flash drive, ma **qualsiasi periferica connessa al computer tramite una porta USB**! È possibile trapiantare un virus da un computer a un altro persino con una macchina fotografica o un lettore MP3.

I trojan sono progettati per essere propagati dagli utenti stessi perché a differenza dei virus propri, essi non possiedono una funzione di proliferazione automatica. Senza saperlo, le vittime dei truffatori portano i trojan da un computer a un altro su chiavette USB. Di conseguenza vengono infettati anche i computer non connessi a Internet e alla rete locale.

Già da un tempo, i cybercriminali organizzati attaccano non solo PC di ufficio, ma anche computer personali dei dipendenti, compresi dispositivi mobili.

Esiste già un trojan bancario studiato per la piattaforma mobile Android — il suo nome è Android.SpyEye.1.

I trojan sono invisibili?

Persiste ancora l'opinione errata e molto imprudente che le attività di un malware sul computer siano ben percettibili e che ci si possa accorgere velocemente se questo sia infetto. Non è per niente vero!

- Lo scopo degli scrittori di virus moderni è creare malware che, dopo aver infettato un computer, devono nascondersi per un tempo più lungo possibile e non essere notati né dall'utente né da programmi speciali (antivirus).
- Per esempio, avviato sulla macchina infetta, Trojan.Carberp intraprende una serie di misure per ingannare i programmi di controllo e sorveglianza. Una volta avviato, il trojan si integra nelle altre applicazioni in esecuzione.

Perché succede?

1. Tutti i programmi malevoli che includono tecnologie complesse e sono stati creati al fine di rubare fondi vengono sottoposti a test chiamati a chiarire se i malware possano essere rilevati dagli antivirus. Di conseguenza, gli antivirus potrebbero non avvistare alcuni programmi malevoli prima dell'arrivo dei relativi esemplari al laboratorio antivirale.
2. Se i malintenzionati sanno esattamente quale antivirus si usa sui computer di una società, i cavalli di troia creati al fine di rubare fondi da questa determinata società possono nascondersi per un tempo abbastanza lungo senza essere individuati dal programma antivirale.
3. Nella storia riferita sopra, il trojan è penetrato sul computer dell'addetta alla contabilità sfruttando alcune vulnerabilità delle applicazioni installate. Quando la dipendente ha premuto sul pulsante nella finestra pop-up, il trojan è stato attivato. Insediatosi nel sistema, il malware ha potuto cominciare a rubare qualsiasi informazione con facilità.
4. Gli utenti stessi — quelli che non conoscono i principi fondamentali di sicurezza informatica — violano le politiche di protezione antivirale involontariamente o per negligenza e facilitano la penetrazione dei virus nella rete locale dell'azienda (per esempio, utilizzano periferiche USB non controllando se portino virus, aprono automaticamente email arrivate da mittenti sconosciuti, navigano su Internet senza alcuni limitazioni durante le ore di lavoro ecc.).

Per combattere l'analfabetismo informatico, Doctor Web crea corsi di formazione progettati per un vasto pubblico e offre gratis prove on-line dedicate alla sicurezza informatica. Le conoscenze

che si possono acquisire con un corso aiutano ad affrontare minacce informatiche e a non cadere in trappole inventate dai cybercriminali.

Progetto formativo WebIQmetro:
http://www.drweb.com/web-iq/

Portale del sistema di formazione di Doctor Web:
http://training.drweb.com

Attenzione!

Oggi l'antivirus è l'unico software che può liberare il sistema operativo da programmi malevoli.

Che fare?

Spesso le vittime si accorgono troppo tardi del furto di denaro, cioè quando il crimine è già stato compiuto. Questo non significa che non rimanga niente da fare! In questo momento, diventa molto importante un'adeguata reazione all'incidente.

Attenzione!

- Non cercate di aggiornare l'antivirus o lanciare la scansione — così si distruggono le tracce degli intrusi nel sistema!
- Non cercate di reinstallare il sistema operativo!
- Non cercate di rimuovere alcuni file o programmi dal disco!
- Non utilizzate il computer da cui si suppone che siano state rubate le informazioni di autenticazione del sistema di home banking — anche se l'uso di questo computer fosse essenziale!

Non esistono informazioni statistiche unificate che si riferiscono ai furti di denaro in sistemi di home banking tramite l'utilizzo di programmi malevoli. Spesso le persone interessate non si rivolgono alla polizia pensando che non sia possibile recuperare i fondi rubati. Le vittime non sanno come comportarsi in una situazione di emergenza e non conoscono la procedura con la quale si può aprire un'inchiesta, così perdono tanto tempo prezioso.

Il furto di fondi con l'impiego di malware è un reato. Per iniziare un procedimento penale contro i cybercriminali, dovete sporgere una denuncia. Probabilmente non siete le uniche vittime dei cybercriminali. È possibile invece che siate le prime persone che informano la polizia del reato informatico, ma in questo modo aiuterete a fermare le attività illegali.

Ogni criminale lascia tracce. Rimangono tracce anche in seguito ai reati informatici — quindi questo male **può e deve essere combattuto**.

Dr.Web S.r.l.

Russia, 125124, Mosca, via 3 Yamskogo Polya, tenuta 2, edificio 12A
Telefono: +7 (495) 789-45-87 (centralino)
Fax: +7 (495) 789-45-97

www.drweb.com | www.av-desk.com | www.freedrweb.com